高等学校计算机科学与技术教材

网络安全与管理

姜文红　编著

清 华 大 学 出 版 社
北京交通大学出版社
·北京·

内 容 简 介

本书介绍网络安全和网络管理两方面的基础知识。在网络安全部分，主要介绍密码编码学和网络安全技术，以及利用安全技术构建安全的内部网络。在网络管理部分，主要介绍简单网络管理协议的基本原理和应用。本书既注重基础理论的详细介绍，又注重结合实际应用进一步巩固和提高理论知识。

本书可作为高等学校计算机专业高年级本科生的教材和教学参考书。

图书在版编目（CIP）数据

网络安全与管理／姜文红编著. —北京：清华大学出版社；北京交通大学出版社，2007.7
（高等学校计算机科学与技术教材）
ISBN 978－7－81082－984－7

Ⅰ.网… Ⅱ.姜… Ⅲ.计算机网络－安全技术－高等学校－教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2007）第 050430 号

策划编辑：韩　乐
责任编辑：方元元
出版发行：清华大学出版社　邮编：100084　电话：010－62776969　http：//www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010－51686414　http：//press.bjtu.edu.cn
印 刷 者：北京东光印刷厂
经　　销：全国新华书店
开　　本：185×260　印张：12.25　字数：303 千字
版　　次：2007 年 6 月第 1 版　2007 年 6 月第 1 次印刷
书　　号：ISBN 978－7－81082－984－7／TP·344
印　　数：1～4 000 册　定　价：20.00 元

前　言

随着互联网应用范围和规模的不断扩大，网络安全的问题日益突出，网络管理也越来越受到人们的重视。为了维护和保障网络系统的安全及网络的正常运行，社会各方面都需要大量的专业人才。因此，各个高校纷纷开设了网络安全与管理方面的课程，旨在培养基础理论扎实，同时又具有一定实际操作经验的学生。但编者在从事专业课的教学过程中，苦于没有合适的专业教材，于是编者从网络信息安全的基本原理和网络管理的基本概念出发，依据网络安全与网络管理技术的发展趋势，结合多年的教学经验和体会，编写了此书。本书适合作为计算机专业本科高年级的专业课教材和教学参考书。

全书分为两大部分，第一部分 1～9 章为网络安全部分，第二部分第 10 章为网络管理部分。

第 1 章是网络安全概述，介绍网络安全的特征、对网络安全造成威胁的因素、安全服务和安全机制、信息系统安全评估标准，以及网络安全的模型。

第 2 章介绍对称密码体制，包括密码学的一些基本概念、古典加密技术、对称密码加密技术等内容。

第 3 章介绍公钥密码体制，包括公钥密码体制的基本原理、典型的公钥密码系统、认证和数字签名等内容。

第 4 章介绍密钥分配技术，包括对称密码体制的密钥分配、公钥密码体制的密钥分配、Diffie-Hellman 密钥交换、X.509 标准和证书，以及公开密钥基础设施（PKI）等内容。

第 5 章介绍电子邮件安全性，包括 PGP 和 S/MIME 两种应用。

第 6 章 IP 安全协议，包括 IPSec 的产生背景、IPSec 的体系结构、IPSec 的实现模式、IPSec 的模块、IPSec 的两种安全机制，以及 IPSec 的密钥管理等内容。

第 7 章介绍安全套接字层和传输层安全，包括安全套接字层的体系结构、修改密码规范协议、报警协议，以及传输层安全等内容。

第 8 章介绍网络安全技术，包括防火墙和入侵检测技术，以及计算机病毒及其防范措施等内容。

第 9 章介绍利用防火墙保护内部网络的方法，包括内部网络中各种服务器的配置方法、具体防火墙的使用方法、交换机和路由器的配置及使用、利用交换机划分 VLAN 等内容。

第 10 章介绍网络管理技术，包括简单网络管理协议 SNMP、RMON 和 CMIS/CMIP，主要重点介绍 SNMP 的管理模型、工作原理、SNMP 的消息类型和运行过程等内容。

每一章后面都有相应的思考题，以此帮助读者复习掌握各章节的内容。

本书在编写过程中，参考了大量文献，在此对各文献的编者表示衷心的感谢。

由于编写时间仓促，以及编者的编写水平限制，本书难免存在错误和疏漏之处，在此恳请各位读者和专家提出宝贵意见，给予批评指正。

编　者

2007 年 6 月于北京

目　　录

第一部分　网 络 安 全

第 1 章　网络安全概述 …… 1
1.1　网络安全的特征 …… 1
1.2　对网络安全造成威胁的因素 …… 2
1.2.1　信息系统的脆弱性 …… 2
1.2.2　安全性攻击 …… 3
1.3　安全服务 …… 4
1.4　安全机制 …… 5
1.5　信息系统安全评估标准 …… 7
1.5.1　各个国家的评估准则 …… 7
1.5.2　我国计算机信息系统安全保护等级划分准则 …… 7
1.6　网络安全模型 …… 7
本章小结 …… 9
思考题 …… 9
第 2 章　对称密码体制 …… 10
2.1　数据加密基本概念 …… 10
2.1.1　什么是密码学 …… 10
2.1.2　密码学发展的历史 …… 10
2.1.3　常用的术语 …… 11
2.1.4　密码体制的分类 …… 11
2.2　古典加密技术 …… 13
2.2.1　数据表示方法 …… 13
2.2.2　凯撒密码 …… 13
2.2.3　单表替代密码 …… 14
2.2.4　多表替代密码 …… 15
2.2.5　一次密码本 …… 16
2.2.6　置换技术 …… 16
2.2.7　简单异或 …… 19
2.3　对称密码加密技术 …… 19
2.3.1　数据加密标准 …… 19
2.3.2　三重 DES …… 24
2.3.3　国际数据加密算法 …… 24
2.3.4　高级加密标准 …… 25
2.4　分组密码的工作模式 …… 28
本章小结 …… 29
思考题 …… 29

第 3 章　公钥密码体制 …… 31
3.1　公钥密码体制的基本原理 …… 31
3.1.1　公钥密码体制的发展 …… 31
3.1.2　公钥密码体制的基本思想 …… 32
3.2　典型的公钥密码系统 …… 33
3.2.1　RSA 系统 …… 33
3.2.2　Diffie-Hellman 系统 …… 34
3.3　认证 …… 35
3.3.1　基于消息加密方式的认证 …… 35
3.3.2　消息认证码认证方式 …… 37
3.3.3　散列函数认证方式 …… 37
3.4　数字签名 …… 42
3.4.1　直接数字签名 …… 43
3.4.2　基于可信任的第三方的数字签名 …… 44
本章小结 …… 45
思考题 …… 45
第 4 章　密钥分配 …… 47
4.1　对称密码体制的密钥分配 …… 47
4.2　公钥密码体制的密钥分配 …… 50
4.2.1　公钥密码体制中公钥的分配 …… 50
4.2.2　利用公钥密码分配对称密码体制的秘密钥 …… 53
4.3　Diffie-Hellman 密钥交换 …… 54
4.4　X.509 标准 …… 55
4.4.1　X.509 证书的格式 …… 56
4.4.2　X.509 证书的取得 …… 56
4.4.3　X.509 证书的撤销 …… 57
4.5　公开密钥基础设施 …… 57
本章小结 …… 58
思考题 …… 59
第 5 章　电子邮件安全 …… 60
5.1　DOS 操作系统下 PGP 软件的使用 …… 60
5.1.1　PGP 的安装 …… 61
5.1.2　PGP 的设定 …… 61
5.1.3　PGP 程序的功能与使用方法 …… 63
5.2　Windows 操作系统下 PGP 软件的使用 …… 69
5.3　S/MIME …… 73
本章小结 …… 75
思考题 …… 76
第 6 章　IP 安全协议 …… 77
6.1　IPSec 的产生背景 …… 77

6.2 IPSec 的应用 …… 78
6.3 IPSec 体系结构 …… 78
6.4 IPSec 的实现模式 …… 79
6.5 IPSec 的模块划分 …… 80
6.5.1 安全关联 …… 80
6.5.2 安全策略数据库和安全关联数据库 …… 80
6.5.3 IKE 模块 …… 81
6.5.4 策略和 SA 管理模块 …… 81
6.5.5 IPSec 模块 …… 81
6.6 IPSec 安全机制 …… 82
6.6.1 认证头 …… 82
6.6.2 封装安全载荷 …… 87
6.7 密钥管理 …… 90
6.7.1 ISAKMP 消息头结构及说明 …… 91
6.7.2 载荷类别及说明 …… 92
6.8 IPSec 的应用前景 …… 93
本章小结 …… 93
思考题 …… 93
第 7 章 安全套接字层和传输层安全 …… 94
7.1 概述 …… 94
7.2 安全套接字层的体系结构 …… 95
7.2.1 SSL 记录协议层 …… 95
7.2.2 SSL 握手协议层 …… 96
本章小结 …… 99
思考题 …… 99
第 8 章 网络安全技术 …… 100
8.1 防火墙技术 …… 100
8.1.1 基本概念 …… 100
8.1.2 防火墙的功能 …… 101
8.1.3 防火墙的分类 …… 101
8.2 入侵检测技术 …… 104
8.2.1 入侵检测技术的分类 …… 104
8.2.2 常用的入侵检测技术 …… 106
8.3 计算机病毒及其防范措施 …… 107
8.3.1 计算机病毒的特点 …… 107
8.3.2 计算机病毒的分类 …… 107
8.3.3 计算机病毒的防治 …… 108
8.3.4 常用的杀毒软件 …… 109
本章小结 …… 113
思考题 …… 114
第 9 章 利用防火墙保护内部网络 …… 115

9.1 内部网络中各种服务器的配置 …… 115
9.1.1 安装 IIS …… 115
9.1.2 Web 服务器的配置 …… 116
9.1.3 FTP 服务器的配置 …… 122
9.1.4 DNS 服务器的配置 …… 125
9.1.5 电子邮件服务器的配置 …… 129
9.2 防火墙的使用 …… 130
9.3 交换机的使用及 VLAN 的划分 …… 139
9.4 路由器的配置使用 …… 147
9.4.1 路由器的配置方式介绍 …… 147
9.4.2 路由器的命令行界面 …… 149
9.4.3 路由器的初始配置 …… 150
9.4.4 显示配置 …… 156
9.4.5 包过滤规则的设计 …… 157
9.4.6 路由器 NAT 规则的配置 …… 162
9.4.7 配置 StoneGate 防火墙 NAT 策略 …… 162
本章小结 …… 166
思考题 …… 167

第二部分 网 络 管 理

第 10 章 网络管理 …… 168
10.1 网络管理概述 …… 168
10.2 简单网络管理协议 …… 169
10.2.1 SNMP 管理模型 …… 169
10.2.2 SNMP 工作原理 …… 171
10.2.3 管理信息库 …… 172
10.2.4 管理信息结构 …… 173
10.2.5 SNMP 消息类型 …… 175
10.2.6 SNMP 消息格式 …… 176
10.2.7 SNMP 的运行过程 …… 177
10.2.8 SNMP 的特点 …… 178
10.2.9 SNMPv3 …… 179
10.3 RMON …… 179
10.3.1 RMON 管理信息库 …… 180
10.3.2 RMON 使用实例 …… 182
10.4 CMIS/CMIP …… 184
本章小结 …… 184
思考题 …… 185
参考文献 …… 186

第一部分　网 络 安 全

第 1 章　网络安全概述

本章要点

- ☑ 了解网络安全的特征
- ☑ 了解对网络安全造成威胁的因素
- ☑ 理解 ISO 7498 标准所确定的安全服务
- ☑ 理解实现安全服务的安全机制
- ☑ 了解世界各国信息系统安全评估的标准
- ☑ 掌握为实现安全通信设计的模型

目前，随着 Internet 越来越深入人们的生活，以互联网为基础的信息时代使人们在享受网络所带来的便利的同时，也充分意识到网络安全的重要性和紧迫性。如何防止网络中机密信息的泄露和篡改，保护网络信息的安全，是迫切需要解决的问题。

本章主要介绍网络安全的特征、对网络安全造成威胁的因素、安全服务、安全机制、信息系统安全评估标准等几方面的内容，从而使人们了解网络信息系统所面临的安全问题。

1.1　网络安全的特征

网络安全从本质上说是网络上信息的安全，也就是保障信息在存取、处理、传输过程中不被非法使用和篡改。国际标准化组织将计算机安全定义为为数据处理系统的建立而采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因遭到破坏、更改和泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全应具有以下 5 个方面的特征。

① 保密性 指信息不泄露给非授权的实体、过程及供其使用的特性。

② 完整性 指信息在存储或者传输的过程中，未经授权不被修改、不被破坏、不丢失的特性，也就是信息从其产生到被利用的过程中保持一致性。

③ 可用性 指授权用户可访问并可按其要求供其使用的特性，也就是信息应能在合法用户所需时刻被存取的特性。

④ 可控性 指授权实体可以随时控制信息的传播和内容的机密性。

⑤ 可靠性 指信息系统能够迅速、准确地为用户提供所需的服务。

1.2 对网络安全造成威胁的因素

1.2.1 信息系统的脆弱性

计算机网络是计算机技术和通信技术相结合的产物，目前，Internet 已经成为在世界范围内人们互相交流沟通的工具，利用网络可以方便地交换信息、共享资源。网络为人们提供了极大的便利，同时也促进了科学技术及文化、经济、社会的快速发展，但是同时也带来了安全方面的问题。由于信息系统本身的脆弱性，为各种网络攻击提供了一定的条件。下面从 3 个方面分析系统脆弱性存在的原因。

首先，从硬件方面来说，各种计算机、网络设备、传输介质及转换器等除了存在设备的自然老化之外，在工作过程中，由于没有安全防范措施、设计缺陷，以及存在电磁辐射等情况，会造成信息被窃听、篡改、泄露。

其次，在于软件方面，计算机软件主要有操作系统和各种通用的应用软件。操作系统和各种应用软件本身在设计和开发过程中，由于人们的认知能力和实践能力有限，不可避免地存在一些错误和缺陷，而且系统越大，越复杂，其安全隐患也越多。例如，微软的视窗操作系统就经常遭受各种攻击，而微软公司也会针对其系统存在的缺陷，不断推出各种补丁程序，对各种攻击进行防范。因此，软件方面存在的安全漏洞会导致系统的整体安全受到威胁。

最后，在网络通信协议方面，Internet 所采用的 TCP/IP (Transmission Control Protocol/Internet Protocol) 协议本身存在安全隐患。要分析 TCP/IP 协议的安全隐患，就要从 Internet 的起源说起。1969 年 9 月，由美国国防部高级研究计划署发起，十几个研究机构和大学一起，研制出了 ARPANET。该网的目的是将若干大学、科研机构和公司的多台计算机连接在一起，实现资源共享。在建网初期，ARPANET 只有 4 个结点，后来规模逐渐扩大。ARPANET 为计算机网络的发展奠定了基础，是计算机网络技术发展的里程碑。自 ARPANET 出现后，世界上许多先进国家纷纷组建了自己的网络，各大计算机公司也纷纷推出了自己的网络体系结构。但是，各个体系结构之间都是各自封闭的。为了使不同体系结构之间的计算机网络能够互连，进一步实现更大范围的资源共享，国际标准化组织 ISO 在 1977 年开始着手研究网络互连问题，并提出了一个能使各种计算机在世界范围内进行互连的标准框架，即开放系统互连参考模型 (ISO/OSI 模型)，但这些标准由于过于复杂和完整，并没有在世界范围内得到广泛应用。20 世纪 70 年代，由于 ARPANET 的发展，并成功地采用了 TCP/IP 协议，使网络可以在 TCP/IP 体系结构和协议的基础上进行互连。1983 年，美国加州大学伯克利分校开始推行 TCP/IP 协议，并以 ARPA 网为主干建立了早期的互联网。1986 年，ARPANET 正式分为两部分 :美国国家基金会 (NSF) 资助的 NSFNET 和军方独立的国防数据网 MILNET。由于美国国家基金会的支持，许多地区和院校的网络开始使用 TCP/IP 协议与 NSFNET 连接，Internet 作为使用 TCP/IP 协议连接的各个网络的总称被正式采用。到了 20 世纪末，互联网的应用越来越普及，随着全世界基础设施的建设，Internet 已经深入到各个角落。

基于 TCP/IP 协议的 Internet 使异型计算机之间、异构网络之间的互连得以实现，极大地推动了互联网在全球范围内的普及。但是人们在享受 Internet 技术带来的便利的同时，认识到 TCP/IP 协议所存在的安全隐患。由于 TCP/IP 协议是在可信任网络环境下开发出来的协

议，所以其设计并未考虑安全问题，当其被推广到世界范围的应用环境之后，其安全性问题就不可避免地对系统的安全性带来影响。

除了以上的各种原因之外，还存在由于黑客及病毒等恶意程序的攻击所带来的问题。

既然系统中存在这样的安全缺陷，一旦这些缺陷被别有用心的人利用，那么就会产生相应的安全威胁。常见的安全威胁有以下几种情况。

① 非授权访问：指非授权用户非法访问或者授权用户超越权限访问。例如，利用一些小工具，窃取用户口令，非法对系统进行操作；或者诱使用户下载一些程序，这些程序一旦启动，就会在用户系统上安装“特洛伊木马”程序，非法获取用户数据等。

② 信息泄露：指敏感信息在有意或者无意中暴露给无权访问该信息的实体。例如，信息在传输过程中丢失或者泄露；通过截获信息，对信息流量、流向、长度等参数进行分析，推测出对其有用的信息。

③ 拒绝服务：指系统或其资源难以或者不能继续服务，其利用价值或者服务能力下降或者丧失。通常是攻击者利用一些专门工具或者特殊手段对网络资源进行抢占，从而造成合法用户无法使用网络。有两方面的原因可以造成拒绝服务这种情况的出现，一是受到攻击；二是由于系统受到破坏而中断服务。

④ 破坏数据完整性：在未授权的情况下对数据进行修改、删除和重放等操作，使数据的完整性受到破坏。例如，对一些重要数据进行篡改或者恶意添加大量无用数据，干扰系统的正常使用。

⑤ 假冒欺骗：未授权的实体假冒另一个不同的实体，使通信的另一方相信其是一个合法的用户，从而非法获取系统的访问权限或者得到额外的特权。例如，假冒主机欺骗合法用户，套取或修改使用权限、口令等信息；假冒管理员查阅秘密文件或者发布命令等。

⑥ 旁路控制：绕过系统的认证机制或者访问控制机制。例如，攻击者利用系统的缺陷或者漏洞，绕过本应发挥作用的访问控制机制渗入到系统内部。

⑦ 窃听：通过搭线或者对电磁辐射进行检测等方法截获机密信息。

1.2.2　安全性攻击

按照 RFC2828 对安全性攻击的分类，安全性攻击分为被动攻击和主动攻击。

1. 被动攻击

被动攻击是在未经用户同意的情况下截获、窃取信息或数据。被动攻击不影响网络的正常工作，不对数据信息作任何修改。信息内容泄漏和流量分析就是被动攻击的例子。攻击者通过搭线和接收信号传输过程中辐射的电磁波，获取系统泄露的消息内容。流量分析通过分析截获的消息，得到消息的真实内容或者通过分析数据包的模式，分析出发送信息的源端和接收信息的目的端的位置、身份、消息的频率和长度等。由于被动攻击不对数据进行修改，所以很难被察觉。加密技术可以有效地预防这种攻击。

2. 主动攻击

主动攻击是指有意对数据流进行篡改或生成伪造的数据流。主动攻击可以分为 4 类：假冒、重放、篡改消息、拒绝服务。

① 假冒：指某个实体伪装成另一个合法的实体，以获得相应的权利。

② 重放：指攻击者将获得的信息复制之后，再次发送，在未授权的情况下进行传输。

③ 篡改消息：指攻击者修改合法消息的一部分或者延迟消息的传输，以产生非授权的效果。

④ 拒绝服务：指通过攻击，使合法用户不能正常或无法使用资源。这种攻击形式可以是对整个网络实施破坏，使网络失效或者使网络过载，以达到降低性能、中断服务的目的；也可以是对某一个特定的目标，使其发往某目的地的所有数据都被禁止。

主动攻击和被动攻击相反。被动攻击虽然难以检测，但可以防止，而防止主动攻击却非常困难。因此，防止主动攻击的重点在于检测并能从攻击所造成的破坏中及时地恢复。检测还可以起到某种威慑的效果，在一定程度上可以防止主动攻击。具体可以采用审计、入侵检测等方法。

1.3 安全服务

为加强网络信息系统安全性和对抗安全攻击所采取的一系列措施称为安全服务。国际标准化组织 ISO 在 1989 年颁布了 ISO 7498-2 标准《信息处理系统开放系统互连基本参考模型第 2 部分——安全体系结构》，确定了开放系统互连参考模型的信息安全体系结构，以及在参考模型内部可以提供标准所规定的安全服务与安全机制的位置。ISO 7498 标准是目前国际上普遍遵循的计算机信息系统互连标准。ISO 7498-2 标准包括 5 类安全服务，即认证、访问控制、数据保密性、数据完整性、不可否认性等。下面详细加以介绍。

1. 认证

通过认证可以保证通信的真实性，可以鉴别通信的对等实体及数据源。通常在连接的初始化阶段，保证通信的实体是其所声称的实体。另外，还要保证该连接不受到假冒的第三方进行非授权传输或接收的干扰。

① 对等实体认证：在面向连接传输时，在建立连接或数据传输阶段，为对等实体提供身份确认。

② 数据源认证：在无连接传输时，为数据的来源提供保证，即保证收到的信息的来源是所声称的来源，但对数据的修改或者复制不提供保护。

2. 访问控制

防止对资源的非授权使用。访问控制服务能够控制哪些资源可被利用、如何利用，以及用于哪些方面。

3. 数据保密性

数据保密性是指防止传输的数据未经授权就被泄漏，其可分为以下 4 种。

① 连接保密性：保护一次连接中所有的用户数据。

② 无连接保密性：对无连接的单个数据块的所有用户数据提供保密性。

③ 选择字段保密性：对一次连接或者单个数据块中被选定的字段提供保密性。

④ 业务流量保密性：防止通过观察业务流量获得有用的保密信息。

4. 数据完整性

数据完整性是指保证接收方收到的数据确实是授权实体所发出的数据。数据完整性既可用于保护整个数据流，又可用于单条消息或消息中选定的部分，其主要分为以下几种。

① 具有恢复功能的连接完整性：对一次连接中所有的用户数据提供完整性保护，检测并试图恢复整个数据序列内存在的修改、插入、删除或者重放。

② 无恢复的连接完整性：与①相同，但不恢复数据原貌。

③ 选择字段连接完整性：对一次连接中传输的单个用户数据块内被选定字段提供完整性保护，并能够判断选定字段是否被篡改、插入、删除或者重放。

④ 无连接完整性：对单个无连接数据块提供完整性保护，并检测接收到的数据块是否被修改。另外，提供有限的重放检测。

⑤ 选择字段无连接完整性：对单个无连接数据块内被选定的字段提供完整性保护，并能确定被选定字段是否被修改。

5. 不可否认性

防止任何一方通信实体否认传输或者接收过某消息。

① 源不可否认：即消息发出后，消息的接收方能够证明消息的确是由所声称的发送方发出的。

② 宿不可否认：即当消息接收后，消息的发送方能够证明消息的确已经被声称的接收方接收了。

安全服务在 TCP/IP 协议栈中实施的位置如表 1-1 所示。

表 1-1　TCP/IP 协议栈可提供的安全服务

安全服务	TCP/IP 协议层			
	数据链路层	网络层	传输层	应用层
对等实体认证	*	√	√	√
数据源认证	*	√	√	√
访问控制	*	√	√	√
连接保密性	√	√	√	√
无连接保密性	√	√	√	√
选择字段保密性	*	*	*	√
业务流量保密性	√	√	*	√
具有恢复功能的连接完整性	*	*	√	√
无恢复的连接完整性	*	√	√	√
选择字段连接完整性	*	*	*	√
无连接完整性	*	√	√	√
选择字段无连接完整性	*	*	*	√
源不可否认	*	*	*	√
宿不可否认	*	*	*	√

√ 表示可以提供此服务，* 表示不能提供此服务。

1.4　安全机制

安全机制是实现安全服务的技术手段，ISO 7498-2 中定义了 8 类安全机制。为了保障系统的安全，可以采用某种安全机制或者多种机制的组合。这 8 种安全机制分别是：加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制和公证机制等。

1. 加密

通过一定的数学算法和加密密钥，将数据变换为不可知的形式。加密算法分为可逆和不

可逆的机制。可逆加密机制包括对称加密(秘密钥)和非对称加密(公开密钥)。对称加密在加密和解密过程中,使用一个密钥。非对称加密使用两个密钥,一个可以公开,而另一个只有密钥的持有者知道。不可逆加密机制可以使用密钥,也可以不使用密钥。不可逆加密机制包括Hash算法和消息认证码。

2. 数字签名机制

数字签名类似于手写的签名,是附加于发送的数据之后的数据,使接收方可以证明数据源和完整性,也可用于签名和验证。因为只有利用签名者的私有信息才能得到签名,所以一旦签名得到验证,就可以证明,只有持有秘密信息(即私有密钥)的一方才有可能产生那个签名。

3. 访问控制机制

对系统资源进行访问控制的各种机制。

4. 数据完整性机制

用于保证单个的数据字段的完整性及数据流的完整性的各种机制。

5. 认证交换机制

通过信息交换保证实体身份的各种机制。例如可利用认证信息或者实体的特征来进行认证交换。

6. 流量填充机制

在真实的数据流中插入若干数据,产生具有欺骗性的数据单元,以防止流量分析的一种安全机制。

7. 路由控制机制

端系统通过动态选择或者按照预先安排的路由,为某些数据选择物理上安全的路线,通过不同的路由建立连接。

8. 公证机制

由能够得到通信实体的信任的第三方来保证实体间数据交换的性能,如数据的完整性、来源、时间等。

在这8种安全机制中,加密机制是应用最广泛的一种机制,可以应用到保密性、完整性、认证等多种服务中。

一种安全机制可以提供一种或多种安全服务,一种安全服务可以由某种安全机制单独提供,也可以由多种安全机制提供。安全机制与安全服务之间的关系如表1-2所示。

表1-2 安全机制与安全服务的关系

机制/服务	认 证	访问控制	数据保密性	数据完整性	不可否认性
加密	√	*	√	√	*
数字签名	√	*	*	√	√
访问控制	*	√	*	*	*
数据完整性	*	*	*	√	√
认证交换	√	*	*	*	*
流量填充	*	*	√	*	*
路由控制	*	*	√	*	*
公证	*	*	*	*	√

√ 表示可以提供,* 表示不能提供

1.5　信息系统安全评估标准

1.5.1　各个国家的评估准则

1. 美国的彩虹系列

1985 年美国国防部计算机安全中心开发出计算机安全标准——可信任计算机标准评估规则 (Trusted Computer Standards Evaluation Criteria Orange Book，TCSEC)，即橘皮书。它是被大家公认的第一个计算机信息系统评估标准。后来美国国防部计算机安全中心更名为国家计算机安全中心 (NCSC)，并将计算机安全方面的文件汇编成册，形成彩虹系列文集，包括其中橘皮书、红皮书和蓝皮书。TCSEC 标准将安全分为 4 个方面：安全政策、可说明性、安全保障和文档，安全级别从高到低分为 A、B、C、D 4 类，每类之下又分为 A1、B1、B2、B3、C1、C2、D 共 7 级。其中，A 级为绝对可信网络安全，B 级代表完全可信网络安全，C 级代表可信网络安全，D 级则意味着不可信的网络安全。

2. 欧洲信息技术安全评估规则

欧洲信息技术安全评估规则 (ITSEC) 由英国、法国、德国、荷兰 4 国在 20 世纪 90 年代提出。它将安全概念分为功能与功能评估两部分，定义了从 E0 级到 E6 级的 7 个安全等级。ITSEC 还定义了 10 种功能，其中前 5 种与橘皮书中的 C 级要求相似。

3. 加拿大可信任计算标准

加拿大政府制定的可信任计算标准 (CTCS) 由两部分组成：加拿大可信任计算机产品评估标准 (CTCPEC) 和普通标准 (CC)。CTCS 1993 年公布了 3.0 版。CTCPEC 把 ITSEC 和 TCSEC的特点相结合，并将安全分为功能性要求和保证性要求两部分。该标准分为 7 个保证级，由低到高依次为 EAL-1 到 EAL-7。

1.5.2　我国计算机信息系统安全保护等级划分准则

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全等级保护系列标准的核心。此标准将计算机信息系统安全性从低到高划分为 5 个等级，分别为：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。计算机信息系统安全保护能力随着安全保护等级的增高逐渐增强。

1.6　网络安全模型

以在 Internet 上通信双方传送消息为例，来讨论建立安全的基本模型。通信双方传递信息的过程是：首先双方要确定从源端到目的端的路由，然后在该路由上采用共同使用的通信协议 (在 Internet 上为 TCP/IP 协议) 共同协商建立一条逻辑信息通道。

在保护信息的传输过程以防止攻击者对信息造成危害时，任何用来保证安全的方法都包含以下两个方面。

① 对发送方要发送的消息进行相关的安全变换，即加密和认证。加密是根据一定的数学算法，将消息变换成攻击者无法读懂的内容。认证是将基于消息的附加内容附在消息后面，用

来验证发送方身份的真实性。

② 通信双方共享的某些秘密信息,如加密所使用的密钥。这些秘密信息只由通信双方掌握,不希望被攻击者获知。

同时,为了实现信息的安全传输,有时需要一个可信任的第三方参与。第三方负责通过可信任的方式,向通信双方分配双方共享的秘密信息或者当通信双方产生争议时进行仲裁。

根据上述几个方面,得到下面的网络通信的安全模型,如图 1-1 所示。

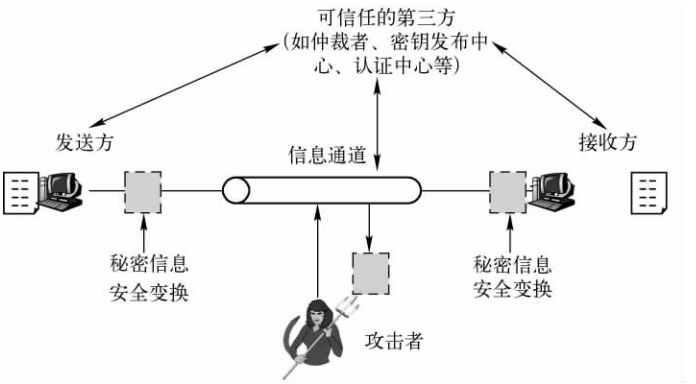

图 1-1 网络通信的安全模型

根据图 1-1 的安全模型,设计一个安全服务应该考虑以下 4 个方面的内容。

① 设计一个进行安全变换的算法,用于对发送的消息进行相关的安全变换,该算法应足够强壮,不易被攻破。

② 生成用于在进行该安全变换算法中进行安全变换的秘密信息,如加密密钥等。

③ 设计通信双方发布和共享秘密信息的方法,如通过可信任的第三方发布等。

④ 确定通信双方所采用的协议,利用安全变换的算法和秘密信息实现安全服务。

对于访问信息系统的情况,由于信息系统是存放和处理信息的场所,其安全要求与以上所讨论的模型不同,在图 1-2 中给出了网络访问的安全模型。其安全要求是保证系统正常工作而不受有害的访问。

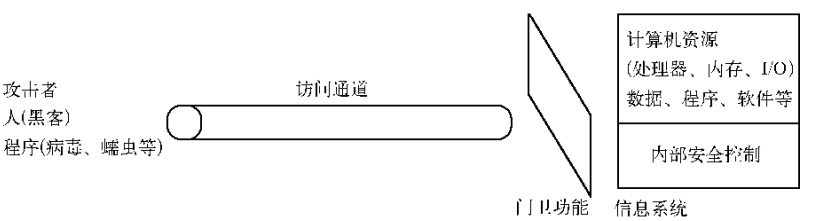

图 1-2 网络访问的安全模型

图 1-2 中所示模型受到的攻击主要有以下两类。

① 信息访问威胁 非授权获取或修改信息。

② 服务威胁 利用系统缺陷破坏系统,禁止合法用户使用资源和服务。

对于这两类威胁,可以通过两种安全机制实现安全服务。第一类称为门卫功能,包括登录

过程只允许授权用户访问，拒绝非授权用户的访问，屏蔽逻辑程序等访问控制机制，以及检测并拒绝蠕虫、病毒等恶意攻击程序访问系统；第二类由内部安全控制部件构成控制机制，包括认证、审计子系统和授权数据库等，负责监视各种活动，分析所存储的信息，检查是否有非法用户或软件获得了访问权，以及检测非法入侵者等。

本章小结

本章主要介绍网络安全所涉及的基础知识，包括网络安全的特征、对网络安全造成威胁的因素、国际标准化组织确定的安全服务和安全机制、信息系统安全评估标准、网络安全模型等内容。

由于网络信息系统本身的脆弱性，造成其容易受到各种攻击。在考虑实施网络安全措施时，应从安全服务的 5 个方面入手，采取 ISO 7498-2 标准中 8 种安全机制中的一种或多种的组合，在 TCP/IP 协议栈的相应各层采取相应的安全机制，以达到相应的效果。在具体实施时，根据实际情况参考网络安全模型，制定相应的安全策略。根据相应的信息系统安全评估标准评估系统的安全等级。

思考题

1. 目前造成计算机网络不安全的原因是什么？
2. 网络安全的含义是什么？
3. 网络安全的特征有哪些？
4. 分析 TCP/IP 通信协议本身存在的缺陷。
5. 简述 ISO 标准中规定的安全服务和安全机制。
6. 简述 OSI 安全服务和安全机制之间的关系。
7. 网络安全所受到的威胁主要有哪些？
8. 主动攻击和被动攻击的区别是什么？
9. 了解世界各国对信息系统进行评估的标准。
10. 校园网经常遭受哪些恶意的攻击？

第 2 章　对称密码体制

本章要点

- ☑ 了解密码学发展的历史
- ☑ 理解密码学中常用的一些术语
- ☑ 掌握单表替代算法的原理
- ☑ 掌握多表替代算法的原理
- ☑ 理解古典加密算法的原理
- ☑ 掌握 DES 算法的计算过程
- ☑ 掌握 IDEA 算法的计算过程
- ☑ 理解 AES 算法的原理
- ☑ 了解分组密码的工作模式

除了物理层的安全之外，几乎所有的安全性都建立在密码学原理的基础之上。基于此，在学习安全性时，首先要详细地学习密码学的基础知识。其中，数据加密是实现网络安全的重要部分，是实现前面第 1 章所介绍的多种安全服务的基础，例如，认证、保密性、完整性及不可否认性等。

本章主要从以下几个方面对数据加密技术进行介绍：数据加密基本概念、古典加密技术、对称密码加密技术和分组密码的工作模式。

2.1　数据加密基本概念

2.1.1　什么是密码学

密码学是研究密码系统的科学，分为密码编码学和密码分析学。密码编码学是研究如何设计密码体制和保密消息的学科；密码分析学是研究如何破译密码体制和解密消息的学科。密码编码学和密码分析学是相互依存、相互支持、密不可分的两个方面。

密码编码学主要有以下几个特征。

① 将消息转换为不易读懂的秘密消息的运算类型：传统的加密算法大多基于替代和置换原理。

② 所使用的秘密消息（密钥）的个数：分为对称密码和非对称密码。

③ 处理消息的方法：分为分组密码和流密码。

2.1.2　密码学发展的历史

最早的数据加密可以追溯到几千年前，那时人们使用象形文字表述意思。后来，人们使用